IEC104 Protocol Stack

User Process	Selected Application Functions
Application Layer (L7)	Selection of Application Service Data Units (ASDU) of IEC 60870-5-101 and 104 Application Protocol Control Information (APCI)
Transport Layer (L4)	Selection of TCP/IP Protocol Suite (RFC 2200) - (X.25, Frame Relay, ATM, ISDN, Ethernet and serial point-to-point (X.21))
Network Layer (L3)	
Link Layer (L2)	
Physical Layer (L1)	

It refers EPA (Enhanced Performance Architecture) stack.

Should Be Known

Controlled Station	Slave (outstation, remote station,RTU,etc.)
Controlling Station	Master station (PC, SCADA etc.)
Monitor Direction	from controlled station (RTU) to the controlling station (PC)
Control Direction	from controlling station (PC) to the controlled station (RTU)
APCI	Application Protocol Control Information
APDU	Application Protocol Data Unit
ASDU	Application Service Data Unit

IEC104 Protocol Application Layer

IEC104 Frame Formats

I-format	It is used to perform numbered information transfer between the controlling and the controlled station.I-format APDUs contains always an ASDU.
S-format	It is used to perform numbered supervisory functions.S-format APDUs always consist of one APCI only.
U-format	U-format is used for activation and confirmation mechanism of STARTDT, STOPDT and TESTFR. - STARTDT and STOPDT are used by the controlling station to control the data transfer from a controlled station. - TESTFR is used by the controlling and/or controlled station to check the status of all established connections to detect any communication problems as soon as possible.

APCI Format

8 bits

Start Byte (0x68)				
Length of APDU				
TESTFR	STOPDT	STARTDT	1	1
				0
Control Field				

U-frame

8 bits

Start Byte (0x68)				
Length of APDU				
			0	1
Recieve sequence no. N (R)				0
Recieve sequence no. N (R)				
Control Field				

S-frame

8 bits

Start Byte (0x68)	
Length of APDU	
Send sequence no. N (S)	0
Send sequence no. N (S)	
Recieve sequence no. N (R)	0
Recieve sequence no. N (R)	
ASDU	
Control Field	

I-frame

Action	Value
Start Data Transfer Activation	0x07
Start Data Transfer Confirmation	0x0B
Stop Data Transfer Activation	0x13
Stop Data Transfer Confirmation	0x23
Test Frame Activation	0x43
Test Frame Confirmation	0x83

U-frame functions and their codes

ASDU Datagram

by Seda Narli

ASDU Format

Type ID	Group
1-40	Process information in monitor direction
45-51	Process information in control direction
70	System information in monitor direction
100-106	System information in control direction
110-113	Parameter in control direction
120-126	File transfer

TypeID	Type Identification	Type of transmission action
SQ	Structure Qualifier	SQ = 0 (sequence of information objects)
		SQ = 1 (just one information object)
T	Test	T=0 (no test)
		T=1 (test)
P / N	Positive / Negative	P/N = 0 (positive confirm) (Command was executed)
		P/N = 1 (negative confirm)
COT	Cause of transmission	COT field is used to control the routing of messages both on the communication network, and within a station, directing by ASDU to the correct program or task for processing. ASDUs in control direction are confirmed application services and may be mirrored in monitor direction with different causes of transmission.
ORG	Originator Address	The originator address is optional on a system basis. It provides a means for a controlling station to explicitly identify itself.
ASDU Address Field	Common Address of ASDU, COA	This is defined as the address of the controlling station in the control direction.

MS	MIN	IV	HOUR	SU	DAY	DOW	MONTH	YEAR
MS : Milliseconds			*IV : Invalid*					
SU : Summer Time			*DOW : Day of Week*					

8 bits

Type Identification		
SQ	Number of objects	
T	P / N	Cause of transmission (COT)
Originator address (ORG)		
ASDU address fields (2 bytes)		
Information object address (IOA) fields (3 bytes)		
Information Elements		
Time Tag (CP56Time)		
Information Object 2		
Information Object N		

Data Unit Identifier

IO 1

Quality Bits		
IV	Valid (0) / Invalid (1)	A value is valid if it was correctly acquired.
NT	Topical (0) / Not Topical (1)	A value is topical if the most recent update was successful.
SB	Not Substituted (0) / Substituted (1)	It means that the value is not derived from the normal measurement.
BL	Not Blocked(0) / Blocked (1)	The value of information object is blocked for transmission.
SPI	Off (0) / On (1)	Single Point Information, SPI=1 means status ON, SPI=0 means status OFF
OV	No Overflow (0) / Overflow (1)	The value of the information object is beyond a predefined range of value (mainly applicable to analog values).
DPI	Double Point Information	indeterminate or intermediate state (0) / determined state OFF (1) / determined state (ON) / indeterminate state (3)
EI	Elapsed time invalid (EI)	This is used with events of protection equipment. If set it means that the elapsed time interval value is invalid.

IOA	The address is used as destination address in control direction and as source address in monitor direction.

IV	NT	SB	BL	0	0	0	SPI

Example of information object Single-point information (SIQ)

Normalized Value (NVA)								
IV	NT	SB	BL	0	0	0	OV	QDS (Quality Descripter)

Example of information object Measured normalized value

by Seda Narli

IEC104 ASDU types and their description

Type	Description	Reference	Format	Valid CoTs
Process Information in Control Direction				
45	Single command	C_SC_NA_1	SCO	6,7,8,9,10,44,45,46,47
46	Double command	C_DC_NA_1	DCO	6,7,8,9,10,44,45,46,47
47	Regulating step command	C_RC_NA_1	RCO	6,7,8,9,10,44,45,46,47
48	Setpoint command, normalized value	C_SE_NA_1	NVA + QOS	6,7,8,9,10,44,45,46,47
49	Setpoint command, scaled value	C_SE_NB_1	SVA + QOS	6,7,8,9,10,44,45,46,47
50	Setpoint command, short floating point	C_SE_NC_1	IEEE STD 754 + QOS	6,7,8,9,10,44,45,46,47
51	Bit string 32 bit	C_BO_NA_1	BSI	6,7,8,9,10,44,45,46,47
Command telegrams with long time tag (7 octets)				
58	Single command with time tag CP56Time2a	C_SC_TA_1	SCO + CP56Time2a	
59	Double command with time tag CP56Time2a	C_DC_TA_1	DCO + CP56Time2a	
60	Regulating step command with time tag CP56Time2a	C_RC_TA_1	RCO + CP56Time2a	
61	Setpoint command, normalized value with time tag CP56Time2a	C_SE_TA_1	NVA + QOS + CP56Time2a	
62	Setpoint command, scaled value with time tag CP56Time2a	C_SE_TB_1	SVA + QOS + CP56Time2a	
63	Setpoint command, short floating point value with time tag CP56Time2a	C_SE_TC_1	IEEE STD 754 + QOS + CP56Time2a	
64	Bit string 32 bit with time tag CP56Time2a	C_BO_TA_1	BSI + CP56Time2a	

Type	Description	Reference	Format	Valid CoTs
System information in control direction				
100	(General-) Interrogation command	C_IC_NA_1	QOI	6,7,8,9,10,44,45,46,47
101	Counter interrogation command	C_CI_NA_1	QCC	6,7,8,9,10,44,45,46,47
102	Read command	C_RD_NA_1	null	5
103	Clock synchronization command	C_CS_NA_1	CP56Time2a	3,6,7,44,45,46,47
104	(IEC 101) Test command	C_TS_NB_1	FBP	6,7,44,45,46,47
105	Reset process command	C_RP_NC_1	QRP	6,7,44,45,46,47
106	(IEC 101) Delay acquisition command	C_CD_NA_1	CP16Time2a	6,7,44,45,46,47
107	Test command with time tag CP56Time2a	C_TS_TA_1		
Parameter in control direction				
110	Parameter of measured value, normalized value	P_ME_NA_1	NVA + QPM	6,7,9,10,20,20+G,44,45,46,47
111	Parameter of measured value, scaled value	P_ME_NB_1	SVA + QPM	6,7,20,20+G,44,45,46,47
112	Parameter of measured value, short floating point value	P_ME_NC_1	IEEE STD 754 + QPM	6,7,20,20+G,44,45,46,47
113	Parameter activation	P_AC_NA_1	QPA	6,7,8,9,44,45,46,47

Type	Description	Reference	Format	Valid CoTs
File Transfer				
120	File ready	F_FR_NA_1	NOF + LOF + FRQ	6,7,8,9,10,44,45,46,47
121	Section ready	F_SR_NA_1	NOF + NOS + LOF + SRQ	6,7,8,9,10,44,45,46,47
122	Call directory, select file, call file, call section	F_SC_NA_1	NOF + NOS + SCQ	5
123	Last section, last segment	F_LS_NA_1	NOF + NOS + LSQ + CHS	3,6,7,44,45,46,47
124	Ack file, Ack section	F_AF_NA_1	NOF + NOS + AFQ	6,7,44,45,46,47
125	Segment	F_SG_NA_1	NOF + NOS + LOS + segment	6,7,44,45,46,47
126	Directory	F_DR_TA_1	NOF + LOF + SOF + CP56Time2a	6,7,44,45,46,47
127	QueryLog – Request archive file	F_SC_NB_1		

by Seda Narli

Type	Description	Reference	Format	Valid CoTs
Process Information in Monitor Direction				
1	Single point information	M_SP_NA_1	SIQ	2,3,5,11,20,20+G
2	Single point information with timetag	M_SP_TA_1	SIQ + CP24Time2a	3,5,11,12
3	Double point information	M_DP_NA_1	DIQ	2,3,5,11,12,20,20+G
4	Double point information with timetag	M_DP_TA_1	DIQ + CP24Time2a	3,5,11,12
5	Step position information	M_ST_NA_1	VTI + QDS	2,3,5,11,12,20,20+G
6	Step position information with timetag	M_ST_TA_1	VTI + QDS + CP24Time2a	2,3,5,11,12
7	Bit string of 32 bit	M_BO_NA_1	BSI + QDS	2,3,5,11,12,20,20+G
8	Bit string of 32 bit with timetag	M_BO_TA_1	BSI + QDS + CP24Time2a	3,5
9	Measured value, normalized value	M_ME_NA_1	NVA + QDS	2,3,5,11,12,20,20+G
10	Measured value, normalized value with timetag	M_ME_TA_1	NVA + QDS + CP24Time2a	3,5
11	Measured value, scaled value	M_ME_NB_1	SVA + QDS	2,3,5,11,12,20,20+G
12	Measured value, scaled value with timetag	M_ME_TB_1	SVA + QDS + CP24Time2a	3,5
13	Measured value, short floating point value	M_ME_NC_1	IEEE STD 754 + QDS	2,3,5,11,12,20,20+G
14	Measured value, short floating point value with timetag	M_ME_TC_1	IEEE STD 754 + QDS + CP24Time2a	2,3,5,11,12,20,20+G
15	Integrated totals	M_IT_NA_1	BCR	2,37,37+G
16	Integrated totals with timetag	M_IT_TA_1	BCR + CP24Time2a	3,37,37+G
17	Event of protection equipment with time tag	M_EP_TA_1	CP16Time2a + CP24Time2a	3
18	Packed start events of protection equipment with time tag	M_EP_TB_1	SEP + QDP +C P16Time2a + CP24Time2a	3
19	Packed output circuit information of protection equipment with time tag	M_EP_TC_1	OCI + QDP + CP16Time2a + CP24Time2a	3
20	Packed single-point information with status change detection	M_PS_NA_1	SCD+QDS	2,3,5,11,12,20,20+G
21	Measured value, normalized value without quality descriptor	M_ME_ND_1	NVA	1,2,3,5,11,12,20,20+G

Type	Description	Reference	Format	Valid CoTs
Process telegrams with long time tag (7 octets)				
30	Single point information with time tag CP56Time2a	M_SP_TB_1	SIQ + CP56Time2a	3,5,11,12
31	Double point information with time tag CP56Time2a	M_DP_TB_1	DIQ + CP56Time2a	3,5,11,12
32	Step position information with time tag CP56Time2a	M_ST_TB_1	VTI + QDS + CP56Time2a	2,3,5,11,12
33	Bit string of 32 bit with time tag CP56Time2a	M_BO_TB_1	BSI + QDS + CP56Time2a	3,5
34	Measured value, normalized value with time tag CP56Time2a	M_ME_TD_1	NVA + QDS + CP56Time2a	3,5
35	Measured value, scaled value with time tag CP56Time2a	M_ME_TE_1	SVA + QDS + CP56Time2a	3,5
36	Measured value, short floating point value with time tag CP56Time2a	M_ME_TF_1	IEEE STD 754 + QDS + CP56Time2a	2,3,5,11,12,20,20+G
37	Integrated totals with time tag CP56Time2a	M_IT_TB_1	BCR + CP56Time2a	3,37,37+G
38	Event of protection equipment with time tag CP56Time2a	M_EP_TD_1	CP16Time2a + CP56Time2a	3
39	Packed start events of protection equipment with time tag CP56time2a	M_EP_TE_1	SEP + QDP + CP16Time2a + CP56Time2a	3
40	Packed output circuit information of protection equipment with time tag CP56Time2a	M_EP_TF_1	OCI + QDP + CP16Time2a + CP56Time2a	3
System information in monitor direction				
70	End of initialization	M_EI_NA_1	COI	4

by [Seda Narli]

Cause of Transmission

Code	Cause of Transmission	Abbreviation
1	periodic, cyclic	per/cyc
2	background interrogation	back
3	spontaneous	spont
4	initialized	init
5	interrogation or interrogated	req
6	activation	act
7	confirmation activation	actcon
8	deactivation	deact
9	confirmation deactivation	deactcon
10	termination activation	actterm
11	feedback, caused by distant command	retrem
12	feedback, caused by local command	retloc
13	data transmission	file
14-19	reserved for further compatible definitions	
20	interrogated by general interrogation	inrogen
21	interrogated by interrogation group 1	inro1
22	interrogated by interrogation group 2	inro2
23	interrogated by interrogation group 3	inro3
24	interrogated by interrogation group 4	inro4
25	interrogated by interrogation group 5	inro5
26	interrogated by interrogation group 6	inro6
27	interrogated by interrogation group 7	inro7

Code	Cause of Transmission	Abbreviation
28	interrogated by interrogation group 8	inro8
29	interrogated by interrogation group 9	inro9
30	interrogated by interrogation group 10	inro10
31	interrogated by interrogation group 11	inro11
32	interrogated by interrogation group 12	inro12
33	interrogated by interrogation group 13	inro13
34	interrogated by interrogation group 14	inro14
35	interrogated by interrogation group 15	inro15
36	interrogated by interrogation group 16	inro16
37	interrogated by counter general interrogation	reqcogen
38	interrogated by interrogation counter group 1	reqco1
39	interrogated by interrogation counter group 2	reqco2
40	interrogated by interrogation counter group 3	reqco3
41	interrogated by interrogation counter group 4	reqco4
…		
44	type-Identification unknown	unknown_type
45	cause unknown	unknown_cause
46	ASDU address unknown	unknown_asdu_address
47	Information object address unknown	unknown_object_address

by Seda Narli

Information Elements

Element Type	Description	Length (B)	Used with the following Information Object Type(s)
Process information in monitor direction			
SIQ	Single-point information with quality descriptor	1	1, 2, 30
DIQ	Double-point information with quality descriptor	1	3
BSI	Binary state information	4	7, 8, 33, 51
SCD	Status and change detection	4	20
QDS	Quality descriptor	1	5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 20, 32, 33, 34, 36
VTI	Value with transient state indication	1	5, 6, 32
NVA	Normalized value	2	9, 10, 21, 34, 48, 110
SVA	Scaled value	2	11, 12, 49, 111
IEEE STD 754	Short floating point number	4	13, 14, 36, 50, 112
BCR	Binary counter reading	5	15, 16, 37
Protection			
SEP	Single event of protection equipment	1	17,38
SPE	Start events of protection equipment	1	18,39
OCI	Output circuit information of protection equipment	1	19,40
QDP	Quality descriptor for events of protection equipment	1	18,19,39,40
Commands			
SCO	Single command	1	45
DCO	Double command	1	46
RCO	Regulating step command	1	47

Element Type	Description	Length (B)	Used with the following Information Object Type(s)
Time			
CP56Time2a	Seven octet binary time	7	4, 6, 8, 10, 12, 14, 16, 17, 18, 19, 31, 32, 33, 34, 36, 37, 38, 39, 40, 103, 126
CP24Time2a	Three octet binary time	3	4, 5, 6, 8, 10, 12, 14, 16, 17, 18, 19, 31, 32, 33, 34, 36, 37, 38, 39, 40
CP16Time2a	Two octet binary time	2	17, 18, 19, 38, 39, 40, 106
Qualifiers			
QOI	Qualifier of interrogation	1	100
QCC	Qualifier of counter interrogation command	1	101
QPM	Qualifier of parameter of measured values	1	110,112
QPA	Qualifier of parameter activation	1	111,113
QRP	Qualifier of reset process command	1	105
QOC	Qualifier of command	1	45, 46, 47, 48, 49, 50
QOS	Qualifier of set-point command	1	48, 49, 50
File Transfer			
FRQ	File ready qualifier	1	120
SRQ	Section ready qualifier	1	121
SCQ	Select and call qualifier	1	122

by Seda Narli

IEC 104 Analysis

Sample 1 :
68 0E 4E 14 7C 00 65 01 0A 00 0C 00 00 00 00 05

LPDU bytes	Explanation
68	Start byte
0E	Length of the APDU = 14 bytes
4E	Send sequence number N(S) LSB, bit 0 = 0 => I-Format
14	Send sequence number N(S) MSB
7C	Receive sequence number N(R) LSB
0	Receive sequence number N(R) MSB
65	Type identification: C_CI_NA_1 (counter interrogation command)
1	Number of objects = 1
0A	Cause of transmission = 10 (activation termination)
0	Originator address = 0
0C 00	Common ASDU address (2 octets) = 12 dec.
00 00 00	Object address (3 octets)
5	Counter interrogation request qualifier = 5 (general counter interrogation)

Sample 3 : 68 04 01 00 7E 14

LPDU bytes	Explanation
68	Start byte
4	Length of the APDU = 4
1	bits 2..7 reserved , bit 0 = 1 and bit 1 = 0 => S-Format
0	reserved
7E	Receive sequence number N(R) LSB
14	Receive sequence number N(R) MSB

Sample 2 :
68 34 5A 14 7C 00 0B 07 03 00 0C 00 10 30 00 BE 09 00 11 30 00 90 09 00 0E 30 00 75 00 00 28 30 00 25 09 00 29 30 00 75 00 00 0F 30 00 0F 0A 00 2E 30 00 AE 05 00

LPDU bytes	Explanation
68	Start byte
34	Length of the APDU = 52 bytes
5A	Send sequence number N(S) LSB bit 0 = 0 => I-Format
14	Send sequence number N(S) MSB
7C	Receive sequence number N(R) LSB
0	Receive sequence number N(R) MSB
0B	Type identification: M_ME_NB_1(measured value, scaled value)
7	Number of objects = 7
3	Cause of transmission = 3 (spontanous)
0	Originator address = 0
0C 00	Common ASDU address (2 octets) = 12 dec.
10 30 00	Object address (3 octets) of first information object
BE 09 00	Scaled value + QDS (quality descriptor) of first information object
11 30 00	Object address (3 octets) of second information object
90 09 00	Scaled value + QDS (quality descriptor) of second information object
0E 30 00	Object address (3 octets) of third information object
75 00 00	Scaled value + QDS (quality descriptor) of third information object
28 30 00 25 09 00	Object address + Scaled value + QDS (quality descriptor) of information object four to seven
29 30 00 75 00 00	
0F 30 00 0F 0A 00	
2E 30 00 AE 05 00	

by Seda Narli

References Book

IEC	International Electrotechnical Commission
IEC104	A part of IEC Telecontrol Equipment and Systems Standard IEC 60870-5 that provides a communication profile for sending basic telecontrol messages between two systems in electrical engineering and power system automation.

APDU	APCI + ASDU
APDU Length	APCI - APCI Header
APDU Length	APDU - APCI Header
IO	Information Object
(SQ=0) IO length (bytes)	APDU_length – ADPU_control_fields (4 bytes) – ASDU_header (6 bytes) – IOA (3 bytes) = APDU_length – 13 bytes
(SQ=1) IO length (bytes)	(APDU_length – ADPU_control_fields (4 bytes) – ASDU_header (6 bytes)) / number_of_objects – IOA (3 bytes) = (APDU_length – 10 bytes) / number_of_objects – 3 bytes
Data Unit Identifier	ASDU - Information Objects

ASDU Type References	
M_	Monitored information
C_	Control information
P_	Parameter
F_	File
_Nx	Not time tagged
_Tx	Time tagged
_xA	Status and normalized, with quality
_xB	Scaled, with quality
_xC	Short floating Point, with quality
_xD	Normalized, without quality
Format	A sequence of information elements that are valid for the given type.
Valid COTs	A list of valid cause of transmission codes associated with this type.

Basic Application Functions	
Data acquisition	Collecting data cyclically, upon change, or upon request
Event acquisition	Events occur spontaneously at the application level of the controlled outstation.
Interrogation	Used for updated the controlling station after an internal initialization
Clock synchronization	After system initialization, the clocks are initially synchronized by the controlling station. After, the clocks are periodically resynchronized by transmission of a clock synchronization command.
Command transmission	Used to change the state of operational equipment (Direct command, Select and execute command)
Transmission of integrated totals	Transmits values that are integrated over a specific time period using two methods: - Freeze-and-Read: acquisition of integrated totals - Clear-and-Read: acquisition of incremental information
Changes in protocol and link parameters	When the link parameters are changed
Acquisition of transmission delay	Needed for time correction

Reference :

http://www.fit.vutbr.cz/research/pubs/tr.en?file=%2Fpub%2F11570%2FTR-IEC104.pdf&id=11570

by Seda Narli